

**Computer and Network Security
Fall Semester 2002**

Solution to Quiz No. 2
August 13, 2002
Time Allowed: 20 Minutes

Name: **SOLUTION**

Total: 20 Points
Questions 1 and 2 carry 5 points each
and multiple choice questions carry
one point each

Question 1:

Encrypt the following plain-text with the given poly-alphabetic cipher of period 3:

Plain-text:

A b i r d i n h a n d i s w o r t h t w o i n t h e b u s h

Key:

 a b c d e f g h i j k l m n o p q r s t u v w x y z

M1: P Q R S T I J K L M N U V W O X Y Z A B C D E F G H
M2: H J K L N Q R S T U V W X Y Z O M E G A P I B C D F
M3: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Remember to do away with spaces when encrypting.

Answer:

M1 →	a	r	n	n	s	r	t	i	h	u	M1 →	P	Z	W	W	A	Z	B	L	K	C
M2 →	b	d	h	d	w	t	w	n	e	s	M2 →	J	L	S	L	B	A	C	Y	N	G
M3 →	i	i	a	i	o	h	o	t	b	h	M3 →	R	R	Z	R	L	S	L	G	Y	S

Cipher-text

PJRZLRWSZWLRABLZASBCLL
YGKNYCGS

Question 2:

Encrypt the following plaintext using a single transposition cipher with the keyword “NED”.
Use “Z” for padding, if required.

A q u i c k b r o w n f o x j u m p e d o v e r t h e l a z y d o g

Answer:

<u> N E D </u>
A Q U
I C K
B R O
W N F
O X J
U M P
E D O
V E R
T H E
L A Z
Y D O
G Z Z

Cipher-text

AIBWOUJEVTLYGQCRNXMDEHA
DZUKOFJPOREZOZ

Circle the Correct Choice

1. The art of breaking ciphers, i.e. retrieving the plaintext without knowing the proper key is called:
a. *Message Authentication* b. *Digital Signature* **c. *Cryptanalysis*** d. *Cryptology*
2. This is a mathematical formula that is easy to work forward but very hard to work backward:
a. *Backdoor* b. *Euler's Totient Function* **c. *Trapdoor*** d. *Logic Bomb*
3. The person who designs cryptographic algorithms and cryptosystems is called a
a. *Cryptanalyst* b. *Cryptologist* **c. *Cryptographer*** d. *Cypherpunk*
4. Generally, asymmetric algorithms are much faster to execute on a computer than symmetric ones.
a. *True* **b. *False***
5. Caesar's cipher is an example of a mono-alphabetic transposition cipher.
a. *False* b. *True*
6. The Scytale cipher is an example of a mono-alphabetic transposition cipher.
a. *False* **b. *True***
7. If the strength of your new cryptosystems relies on the fact that the attacker does not know the algorithm's inner workings, you are sunk. This principle is called:
a. *Al-Kindi's Rule* b. *Ceaser's Principle* c. *Scytale's Algorithm* **d. *Kerchoff's Pricniple***
8. Concatenation of various ciphers is called:
a. *Poly-alphabetic cipher* b. *Polymorphic cipher* **c. *Product cipher*** d. *Sum cipher*
9. Which of the following is not a constituent of a cipher mode?
a. *Feedback* b. *Simple Operation* c. *Encryption Algorithm* **d. *Noise***
10. To encrypt 1 MB of plain-text using a One Time Pad (OTP) how long a truly random key would be required?
a. *64 bits* **b. *1 MB*** c. *10 MB* d. *128 bits*